

العنوان:	جرائم الحاسوب و أساليب مواجهتها
المصدر:	الأمن والحياة (أكاديمية نايف العربية للعلوم الأمنية) - السعودية
المؤلف الرئيسي:	محمد، سليمان مصطفى
المجلد/العدد:	مج 18, ع 199
محكمة:	لا
التاريخ الميلادي:	1999
الشهر:	أبريل / ذو الحجة
الصفحات:	49 - 51
رقم MD:	486436
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	العالم العربي، الحاسبات الإلكترونية، جرائم المعلومات، الجرائم الإلكترونية، البرامج الإلكترونية، أمن المعلومات
رابط:	http://search.mandumah.com/Record/486436

© 2016 دار المنظومة. جميع الحقوق محفوظة.
هذه المادة متاحة بناء على الإتفاق الموقع مع أصحاب حقوق النشر، علما أن جميع حقوق النشر محفوظة. يمكنك تحميل أو طباعة هذه المادة للاستخدام الشخصي فقط، ويمنع النسخ أو التحويل أو النشر عبر أي وسيلة (مثل مواقع الانترنت أو البريد الالكتروني) دون تصريح خطي من أصحاب حقوق النشر أو دار المنظومة.

ـ عندما نتحدث عن الحاسوب أو الحاسب الآلي أو الكمبيوتر نعني بذلك جهاز الكمبيوتر من حيث النواحي المادية (Hardware) والنواحي غير المادية (Software) ونلاحظ الحاسوب من الأجهزة التي يجرى عليها الاحلال والتطوير بشكل متسارع الخطى في عالم التكنولوجيا ونجد أن تطور الجريمة بذات التسارع في كثير من الدول. رغم الضمانات الفنية والتأمينات التقنية تعرض الحاسب الآلي أكثر من مرة لاختراق تأمينه ولم يكتف المجرمون والمحترفون في هذا المجال بسرقة الأجزاء المادية (Hardware) وسرقة البرامج (Software) والمعلومات والبيانات (Information & Data) أو سرقة الأموال باستخدام الحاسوب ولكن امتد الإجرام إلى اختراق الشبكات العسكرية واستراتيجيات قومية وتأثير ذلك في حالة الاستعدادات العسكرية وتنفيذ الخطط والبرامج السرية للدول والشركات والمؤسسات.



مقدم سليمان مصطفى محمد *

جرائم الحاسوب وأساليب مواجهتها

ـ ويمكن تعريف جرائم الحاسوب كالآتي :

ـ جريمة الحاسوب هي الجريمة التي يتم ارتكابها إذا قام شخص ما بطريقة مباشرة أو غير مباشرة في استغلال الحاسوب أو تطبيقاته بعمل غير مشروع وضار للمصلحة العامة ومصلحة الأفراد (خاصة).

ـ ومن أمثلة هذه الجرائم سرقة الأموال النقدية، والسلع، والبرامج والبيانات، تدمير البيانات، أو ملفات محددة، اختراق الشبكات وكشف المعلومات أو الأسرار، أو استغلال وقت الحاسوب بشكل غير قانوني ودائماً فإن محترفي جرائم الحاسوب هم من الذين لهم دراية بالنواحي الفنية عن الحاسوب، وتكلف خسائر جرائم الحاسوب مبالغ طائلة جداً وقد قدرت الخسائر في الولايات المتحدة ما بين ٣ ـ ٥ ملايين دولار سنوياً وقد قدرت المباحث الفيدرالية الأمريكية (F.B.I) في نهاية الثمانينيات أن جريمة الحاسوب الواحدة تكلف ٦٠٠ ألف دولار سنوياً في الوقت الذي تكلفه السرقة الواحدة تحت تهديد السلاح حوالي ٣ ألف دولار في دراسة أجراها أحد مكاتب المحاسبة الأمريكية منها الآن ٢٤٠ شركة أمريكية وقعت ضحية جرائم الغش التجاري باستخدام الحاسوب (Computer Fraud).

في دراسة أجريت في المملكة المتحدة ما يقرب ٢١٢ جريمة من جرائم الحاسوب قد تم ارتكابها وأكثر هذه الجرائم تنتج من سوء استخدام البرامج التي تنفذ الإجراءات المطلوبة باستخدام الحاسوب أو إلى سوء تغذية الأجهزة ببيانات غير صحيحة.

أنواع جرائم الحاسوب :

ـ ويمكن تقسيم جرائم الحاسوب إلى خمس مجموعات :

ـ المجموعة الأولى : تشمل الجرائم التي تتمثل في اختراق الحاسوب لتدمير البرامج والبيانات الموجودة في الملفات المخزنة بالحاسوب وهذه هي من أخطر أنواع الجرائم.. وهنا يقوم شخص متخصص بوضع أمر معين (Command) لبرامج الحاسوب وعند تنفيذ هذا الأمر يتم مسح كلي أو جزئي للملفات المرتبطة بهذه البرامج ويتم هذا النوع من الجرائم بقصد أو نية.

ـ المجموعة الثانية : وتتمثل في الجرائم التي تتم بها استغلال البيانات المخزنة على الحاسوب بشكل غير قانوني، ومن أمثلتها الدخول إلى شبكة الحاسوب التي تحمل أرقاماً سرية محددة من خلال استخدام الحاسوب للحصول على مبالغ نقدية تحت هذا الرقم أو الاختراق لكشف الأسرار أو أغراض أخرى.



- المجموعة الثالثة : تشمل الجرائم التي تتم باستخدام الحاسوب لارتكاب جريمة معينة أو التخطيط لها.

- المجموعة الرابعة : وتشمل الجرائم التي يتم استخدام الحاسوب بشكل غير قانوني من قبل الأفراد المرخص لهم باستخدامه، ومن أمثلة ذلك استخدام الموظفين أو العاملين بمركز الحاسوب للأجهزة بعد أوقات العمل الرسمية أو اثناءه مثل استخدامه في التسلية ببرامج الالعاب أو بعض الأغراض الشخصية غير المرتبطة بالعمل الرسمي أو استخدام عشوائي لمفاتيح الأوامر من الذين لا يفهمون الحاسوب وهذا النوع أكثر الجرائم شيوعاً في الدول العربية.

- المجموعة الخامسة : وتتمثل في فيروسات الكمبيوتر والفيروس ماهو إلا برنامج آخر موجود على الكمبيوتر يهدف إلى إصابة الكمبيوتر لإتلاف البرامج وربما كان السبب في ازدياد الرعب من الفيروس هو التزايد الهائل في حجم الاعتماد على أجهزة الكمبيوتر وشبكاتها والخدمات العامة التي توفرها والتي تتبدى في البريد الإلكتروني ومراكز الحاسوب بالمصالح العامة والخاصة ودائماً ما ينتقل الفيروس عند استخدام وسيط تخزيني ملوث بفيروس من فيروسات الحاسوب (Storage Media) وعند إدخال الوسيط وتحميل البيانات (Loading Data) على الحاسوب يتم تدمير البيانات أو تعطيل إستخدام البرامج الأصلية المخزنة على الحاسوب وقد يصدف إرسال مجموعة أسطوانات من جهة بالبريد ويكتشف بأن تكون ملوثة بفيروس لذا يفضل تجربة هذه البيانات قبل تخزينها على الحاسوب الرئيسي وبعض الفيروسات موجود أصلاً بالجهاز ولكن تنشط من وقت لآخر عند تنفيذ بعض الأوامر أو الألعاب.

- وعموماً تتقاسم كل الفيروسات الصفات الآتية :

- خاصية التسلل والعمل في الخفاء (Stealth).

- خاصية التكاثر (Replication) ويعني بأن يصيب الفيروس جهاز الكمبيوتر يقوم بنسخ نفسه عدة مرات بهدف الإنتشار والالتصاق في الملفات المتناثرة على الاسطوانة.

- خاصية التخزين في برامج بدء التشغيل (Boot Sector) وهذه من الفيروسات الذكية تقوم بنسخ نفسها في جزء من الاسطوانة المخصصة لتخزين برامج بدء التشغيل لتسهيل فرص الإصابة، وبعضها تتكاثر في الذاكرة (Ram).

- ويمكن تحديد الجناة (مرتكبي جرائم الحاسوب) إلى خمس مجموعات رئيسية.

١ - الموظفون العاملون بمراكز الحاسوب وهؤلاء يمثلون الغالبية العظمى من مرتكبي جرائم الحاسوب وذلك لسهولة إتصالهم بالحاسوب.

٢ - الموظفون الساخطون على مؤسساتهم الذين يعودون لمواقع العمل بعد فترات العمل الرسمية اما لغرض سرقة المعلومات أو بغرض التخريب.

٣ - فئة العابثين (Hachers) هم الذين ليس لديهم سلطة استخدام الحاسوب ولكنهم مغرمون بالعبث وهم يستخدمون الحاسوب من أجل التسلية وليس بغرض التخزين وغالباً ما يكون من هواة الكمبيوتر.

٤ - الفئة التي تعمل في مجال الجريمة المنظمة باستخدام الحاسوب حيث يقوم هؤلاء باستخدام الحاسوب في شكل غير قانوني في معرفة بعض الأشياء المتعلقة بالأساليب الأمنية المتبعة لتامين المؤسسات التي يسطون عليها.

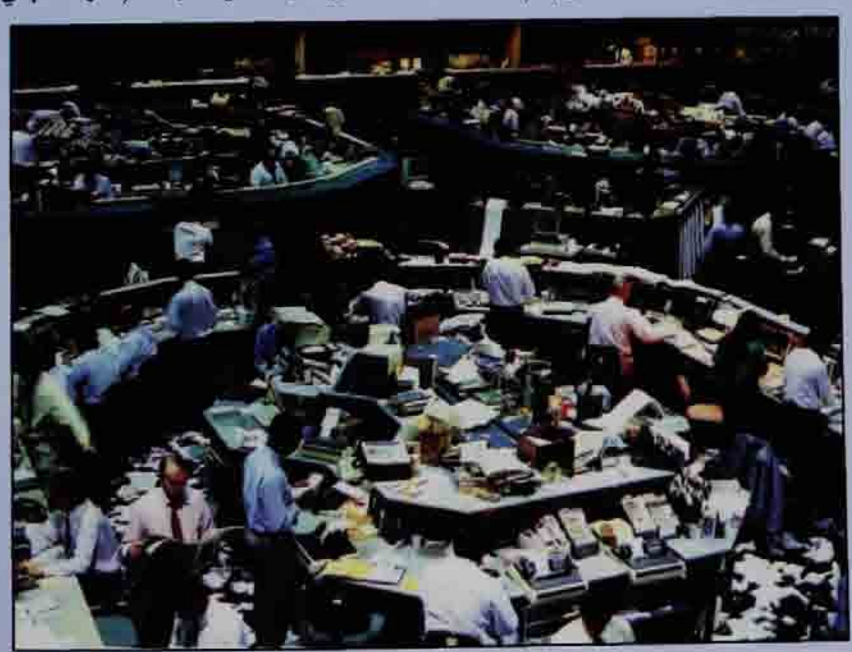
٥ - فئة صانعي وناشري الفيروسات (Solution of Computer Criminal "Viruses")

- ويتم حدوث جرائم الحاسوب في المراحل الآتية :

- مرحلة إدخال البيانات : تحدث الجريمة اذا قام المستخدم بتزوير أو تغيير (فبركة) البيانات ومثال لذلك اذا استطاع الجاني الوصول إلى البيانات المتعلقة بفاتورة الهاتف قبل إعدادها بشكلها النهائي من قبل شركة الهاتف، وتمكن من حذف بعض المكالمات المكلفة من الفاتورة قبل إرسالها له بالبريد أو اثناء قيام أحد مدخلي البيانات تغيير الإجراءات الهجرية أو المستندات الثبوتية لشخص ما أو قام الجاني بتغيير معلومات شخص مشتبه (محظور).

- مرحلة تشغيل البيانات: فإن مرتكبي هذه الجرائم يقومون بتعديل البرامج الجاهزة (Software) التي تقوم بتشغيل البيانات للوصول إلى نتائج محددة أو مقصودة من قبل الجاني..

وفي هذه الحالة يجب أن يكون



الجاني على قدر من الدراية والمعرفة بالنظام.

- مرحلة إخراج البيانات وهي أكثر المراحل التي تنتشر فيها جريمة الحاسوب وتتم في هذه المرحلة سرقة المعلومات أو البيانات المتعلقة بالرقابة على المخزون في إحدى المصالح أو إفشاء بعض المعلومات الخاصة بالإجراءات الأمنية خاضعة للفحص السري لتأمين وضع معين عند موقف معين عند السلطات العسكرية أو أي معلومات بالوزارات أو بالشركات أو الأفراد.

- أساليب تلافي جرائم الحاسوب (Computer Security)

- تتراوح أنواع الحماية من مجرد إحكام اقفال الأماكن التي يوجد بها الحاسوب إلى مجموعة من الطرق التي تستخدم لتشفير البيانات بطريقة لا تمكن الآخرين من اختراق شبكاته وقراءة بياناته والدخول إليها والتلاعب بها.

- وبما أن الحاسوب يشتمل على جانبين مادي (Hardware) وغير مادي (Software) فإن الحماية يمكن تقسيمها إلى أمان مادي لمكونات الأجهزة وأمان غير مادي للبيانات والبرامج (Programs and Data) ويتمثل الأمان المادي في حماية مكونات الحاسوب المادية من أخطار القوى الطبيعية ومن الأخطار الناجمة عن تصرفات الإنسان (Man-Made-Damage) ويمكن تحقيق التأمين المادي من خلال :

- وضع مجموعة من الإجراءات والضوابط تمنع الأفراد غير المصرح لهم باستعمال الحاسوب من دخول مراكز الحاسوب بحيث يوضع الحاسوب الرئيسي في حالة الشبكات (Main Frame) أو الـ (File Server) في مواقع تحميه من الهجوم المادي والتحكم في الدخول إلى أماكن وجوده ومن أدق سبل ضبط الدخول والخروج لمراكز الحاسوب، استخرج البصمات الصوتية وبصمات الأصابع للأشخاص المصرح لهم بالدخول أو إستعمال شبكة العين (Retina) وتتم مضاهاتها مع الشخص الداخل باستخدام وسائل أتوماتيكية سريعة.



- حماية برامج الحاسوب بعمل نسخ احتياطية من البرامج باستخدام الوسائل التخزينية التي تحفظ البرامج والملفات المختلفة لاستخدامها في حالات تلف وسائط التخزين الأصلية أو حدوث أي حذف من اجزاء البرامج أو كلها.

- إحكام أقفال الأمان التي يوجد بها الحاسوب.

- حماية الحاسوب من النيران وأخطار المياه والرياح والحرارة.

وتختلف أساليب مواجهة جرائم البرامج والبيانات بعض الشيء عن أساليب مواجهة جرائم الجزء المادي لأنه من المنطقي أن يظل الحاسوب متاحاً لمستخدميه معظم الوقت أن لم يكن طوال الوقت. وعليه من الضروري حماية البرامج الجاهزة (Software) والمعلومات أو البيانات (Informations of Data) ضد الجرائم المختلفة ومع التطور السريع في صناعة الحاسبات وإنتاج البرامج الجاهزة والوسائط التخزينية المتوفرة بكم هائل من البيانات والمعلومات التي يتم تداولها من خلال مراكز الحاسوب.

ومن أنسب السبل والوسائل لحماية البيانات (شفرة) للإتصال والدخول إلى الحاسوب (Access Code) مثل استخدام الأرقام التي تعطيها البنوك للعملاء والشركات لمستخدميها عند سحب الأموال من حساباتهم بنظام بطاقات الائتمان الممغنطة.

والبطاقات التي يتم استخدامها لحساب وقف استخدام الحاسوب من قبل الأفراد حتى يمكن تحاشي سرقة الأموال ووقف الحاسوب.

- استخدام كلمة مرور (Pass Word) أو كلمة السر وهي عبارة عن كلمة أو عدة أرقام تتم تغذية الحاسب الآلي بها ولا يعرفها إلا مستخدمها.

- أمن المعلومات في الحاسب الآلي :

- نعني بأمن المعلومات في الحاسب الآلي حماية المعلومات من الاطلاع عليها بواسطة أشخاص غير مأذون لهم وتأمين هذه المعلومات للتعامل معها بواسطة الأشخاص المأذون لهم متى ما أرادوا، أن طرق مراجعة البيانات والحماية المعقدة وبرامج الحاسب الآلي التخزينية والأمنية وقوانين الدول لا تستطيع وحدها تأمين المعلومات في الحاسب الآلي. وأن مثل وأخلاق وأمانة العاملين في حقل الحاسب الآلي وضماناتهم على الأنظمة التي يتعاملون بها من أهم عوامل ومؤثرات تأمين المعلومات وعلى كل العاملين بالحاسبات الآلية مراجعة إلتزام بأخلاق المهنة من حين لآخر.■

---

* وزارة الداخلية السودانية - إدارة الحاسوب والمعلومات.